UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

14 M 364

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 30 SIDNEY PLACE, BROOKLYN, NY 11201 AND ANY CLOSED CONTAINERS AND CLOSED ITEMS FOUND THEREIN	**TO BE FILED UNDER SEAL** AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, BRENT TALAGA, being duly sworn, depose and say:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been employed by HSI since 2009. During my tenure as a Special Agent, I have conducted and participated in numerous investigations of criminal activity including, but not limited to, violations of federal criminal law relating to child exploitation as well as the illegal production, distribution, receipt and possession of child pornography. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my work on these cases and in these trainings, I have reviewed multiple examples of child pornography (as that term is defined in 18 U.S.C. § 2256) in all forms of media, including computer media. In the course of my investigations, I have also interviewed people involved in the distribution, sale, production and possession of child pornography and assisted in the execution of search warrants relating to these cases.

2. I have participated in the investigation of this matter. I am familiar with the information contained in this affidavit based on my own personal participation in the

investigation, my review of documents, conversations I have had with other law enforcement officers about this matter, my training and experience, and numerous discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search 30 SIDNEY PLACE, BROOKLYN, NY 11201, described in Attachment A, and any closed containers and closed items found therein (the "SUBJECT PREMISES"), I have not included the details of every aspect of this investigation. Where actions, conversations, and statements of others are described in this affidavit, they are described in substance and in part, except where otherwise indicated.

3. I respectfully submit this affidavit, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, in support of an application for a warrant to search the SUBJECT PREMISES, as described below. The instant investigation, described more fully below, has revealed that an individual, using a publicly available peer-to-peer file sharing program described in more detail below (the "P2P Program"), was engaged in the distribution and possession of child pornography. Further investigation has revealed that the IP Address associated with the user of the P2P Program is registered to an Internet Service Provider customer using the SUBJECT PREMISES as an address. Based on the facts set forth in this affidavit, there is probable cause to believe that there is presently located at the SUBJECT PREMISES evidence and instrumentalities of violations of federal law, including violations of Title 18, United States Code Sections 2252 and 2252A, involving child exploitation offenses. Such evidence may consist of the items set forth in ATTACHMENT B to the proposed Search Warrant. In addition, such evidence may be stored in secure

locations like safe deposit boxes, safes, key-lock strong boxes, and other types of locked or closed containers in an effort to prevent the discovery or theft of said items.

THE SUBJECT PREMISES

4. HSI agents have personally visited and observed the SUBJECT PREMISES and the surrounding area, as recently as April 10, 2014. Based on my discussions with them and their observations of the SUBJECT PREMISES, I have learned, among other things the following:

a. The SUBJECT PREMISES is located on Sidney Place between State Street and Aitken Place in Brooklyn, New York.

b. The SUBJECT PREMISES is a single-family, three-story, light tan brownstone home located at 30 Sidney Place in Brooklyn, New York. Attached as Exhibit 1 is a photograph another HSI agent took of the front of residence.

c. The entrance to the SUBJECT PREMISES is located on the right side of the home off of the street level via stairs. The door entrance consists of two large glass doors. "30 Sidney Place" is written on a plaque in script to the left of the doors.

APPLICABLE DEFINITIONS

5. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," and "visual depiction," as used herein, are defined as set forth in 18 U.S.C. § 2256.

b. The term "child pornography," as used herein, refers to a visual depiction of a minor involved in sexually explicit conduct as defined in 18 U.S.C. § 2256(8)(A), (B) and (C).

c. The term "computer," as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

d. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

PEER-TO-PEER FILE SHARING

6. The present investigation was initiated as a result of the law enforcement community's ongoing concern related to the escalating prevalence of the distribution of child pornography via "Peer-to-Peer" (also known as "P2P") file-sharing software. "Peer to Peer" or "P2P" is a type of file-sharing program that allows people to exchange documents and files between computers. Users of P2P software programs, many of which are available for free on the Internet, can use the programs to transfer files from one computer system to another while connected to the Internet. When installed, a P2P software program allows the installer to designate certain files to share, generally placed in a "shared folder." The files

located in the "shared folder" are accessible to anyone who uses the same program by simply searching for specific files and downloading the files. In this manner, P2P file-sharing software programs allow groups of computers using the same file sharing network to connect directly with each other and to share files from one another's computer systems. As further detailed below, P2P software, such as "Limewire," "EMule," and "Frostwire" are often used to exchange images of child pornography.

7. The Peer-to-Peer file-sharing software programs operate on Peer-to-Peer networks, such as Gnutella or eDonkey (the "P2P Networks"). Upon enabling a P2P Network on one's computer, that computer becomes both a client and a server in the network and is able to share desired files that have been placed in a user's "shared folder" with other P2P networks users and view files made available for sharing by other P2P network users. The P2P software programs mentioned above connect to the P2P Networks and facilitate the trading of images, videos and other files. The software allows the user to search for pictures, movies and other digital files by entering text as search terms. For example, an individual looking for music files by a specific artist may enter a search term such as "Sinatra," and will receive nearly instantaneously a list of other P2P Network users that have music titles pertaining to music artist Frank Sinatra on their hard drives that have been made available to others on the P2P Network.

8. Because of their relative ease of use and perceived anonymity, P2P Networks provide readily available access to child pornography. I know from using the P2P file-sharing software that the search results presented to the user allow the user to select a file and then receive that file from other users around the world. These users can receive the selected file from numerous sources at once. The software can balance the network load and

recover from network failures by accepting pieces of the selected file from different users and then reassembling the selected file on the local computer.

9. P2P networks can only succeed in reassembling a selected file from different parts if the parts all come from the exact same file. For instance, multiple persons sharing one movie can deliver different pieces of that movie to the local software and that local software can reassemble a complete and exact copy from the parts. In fact, the local software can reassemble a complete set of the movie even if the different copies of the same movie from which the local computer draws the parts of the movie have different file names.

10. The P2P software determines whether files with different names are actually the same file based on "hash values." In order for the P2P networks to accomplish the reassembly of files described above, the files being shared on the P2P network are processed through the client software and as part of this processing, a hashed algorithm value ("hash value") is computed for each file being shared, which uniquely identifies it on the P2P Network. A file processed by this hash algorithm operation results in the creating of an associated hash value often referred to as a digital signature, akin to a fingerprint. P2P software uses these hash values to determine whether files hosted on different computers with different names are, in fact, the same file.

11. By querying the P2P networks, I am able to compare the offered hash values with hash values that belong to movies or images of known child pornography. These known movies or images of child pornography have been compiled by law enforcement agencies during the course of separate and unrelated Internet child sexual exploitation investigations into a database readily accessible for law enforcement use. Once a matching set of hash values is identified, an investigator then uses publicly available software to view a

list of network computers/users that are reported to have the same images available for distribution. This process allows an investigator to identify known images of child pornography, including movie files, that are publicly available on the P2P networks.

12. Computers utilizing the Internet identify each other by IP address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet Service Provider company and that company can typically identify the account that uses the IP address to access the Internet.

13. In addition, in some instances, a user of a P2P network has a Global Unique Identifier ("Unique ID"), which is a series of numbers uniquely associated with the software program the user uses to access the network. Provided that the user continues to access the network using the same software program, the user continues to have the same Unique ID, even if the user's IP address changes.

14. One method employed by law enforcement agents to investigate crimes involving child pornography involves the use of an Investigative Software (the "IS") which is currently used in P2P file-sharing investigations to directly download files of child pornography from P2P network users. The IS is designed to "direct connect" to one IP address and browse or download from one specific P2P network user at a time. The IS locates files containing child pornography made available by P2P users by conducting searches for hash values of child pornography images and videos that have been identified as a result of other investigations.

THE INVESTIGATION

15. On or about March 24, 2014, an HSI investigator logged in to ARES, a P2P network, using IS software. The IS located a computer using the IP address 72.229.105.108 ("IP Address 1") that was using the P2P network to make available certain files with file names that contained words generally known to be associated with child pornography images and videos.

16. Using the IS and P2P network, the HSI investigator downloaded two files from the computer at IP Address 1:

a. **babyj-fuck me!** is a video approximately 2:20 minutes long showing an adult male penetrating a pre-pubescent female vaginally.

b. **22.mpg** is a video approximately 4:39 minutes long showing two pre-pubescent girls naked in a bathtub using their hands on an adult male's penis.

17. Open source database searches revealed that IP Address 1 was registered to Time Warner Cable.

18. Records obtained from Time Warner Cable in response to a subpoena showed that, as of April 7, 2014, IP Address 1 was subscribed to "JOANNA ROBINSON." The address associated with IP Address 1 was the SUBJECT PREMISES. There was no indication in the records from Time Warner that the SUBJECT PREMISES was divided into multiple units.

19. Records obtained from Con Edison indicated that, since June 2004, the utilities account was in the name of "JOANNA ROBINSON" and the address was the SUBJECT PREMISES. No other individuals had a utilities account associated with the

SUBJECT PREMISES, and there was no indication in the records from Con Edison that the SUBJECT PREMISES is divided into multiple units.

20. On or about April 10, 2014, two HSI agents spoke with a male individual outside of the SUBJECT PREMISES. The HSI agents stated, in sum and substance, that they were looking for Pakistani males in the neighborhood who were committing identity theft. The individual stated, in sum and substance, that he was a foreign exchange student who lived at the SUBJECT PREMISES. He further stated that JOANNA ROBINSON and her husband owned the entire building. In addition, he stated that the ground-level floor was the children's play area and that he entered the residence through the ground-level entrance, i.e. not the entrance at the top of the stairs in Exhibit 1, but the entrance through the gate and under the stairs.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

21. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

22. I know that collectors of child pornography typically retain their materials and related information for many years.

23. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

24. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

25. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

26. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle"

or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentality of a crime.

SEARCH PROCEDURES TO BE EMPLOYED

25. In searching for data capable of being read, stored, or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the SUBJECT PREMISES, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will search and seize any computers, computer equipment and storage devices and transport these items to an appropriate law enforcement laboratory for review as to whether these items contain contraband. Because of the lengthy period of time necessary to perform a complete search of all material contained in any computers, computer equipment and storage devices, it would not be feasible to conduct this search on the SUBJECT PREMISES, and seizure is necessary so that the preservation of data is not jeopardized. The computers, computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

b. If the computer personnel seize computer devices, the computer personnel will search the computer devices within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted,

it is determined that a computer device contains any data listed in Attachment B, the Government will retain the computer device. If it is determined that the computer devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), such materials and/or equipment will be returned within a reasonable time, not to exceed 60 days from the execution of this warrant, unless further application is made to the Court.

c. The analysis of electronically-stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

26. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the offense specified above.

27. In searching the data, the computer personnel may examine all of the data contained in the computers, computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set

forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit.

28. In order to search for data from computers, computer equipment and storage devices, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. any computers, computer equipment and storage device capable of being used to commit, further or store evidence of the offenses listed above;

b. any computers, computer equipment and storage device used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical discs, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, cameras, Web Cams, and videocameras;

d. any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices, or data; and

g. any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

29. In addition, law enforcement personnel will need to seize and search any device that can capture or store a photographic or video image.

CONCLUSION

30. Based upon the above information, I believe that probable cause exists to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A, involving child exploitation offenses, exists and is concealed on the SUBJECT PREMISES.

31. In consideration of the foregoing, I respectfully request that the Search Warrant sought in this affidavit issue pursuant to Rule 41 of the Federal Rules of Criminal Procedure, permitting authorized agents or officers to enter the SUBJECT PREMISES and therein to search for and seize the items listed in Attachment B to the Search Warrant.

32. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the SUBJECT PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

Brent Talaga

BRENT TALAGA
Special Agent
Homeland Security Investigations

Sworn to before me this
16th day of April, 2014

HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched is **30 Sidney Place, Brooklyn, New York 11201 (the "SUBJECT PREMISES")**, located on State Street and Aitken Place in Brooklyn, New York, further described as:

The SUBJECT PREMISES is located on Sidney Place between State Street and Aitken Place in Brooklyn, New York.

The SUBJECT PREMISES is a single-family, three-story, light tan brownstone home located at 30 Sidney Place in Brooklyn, New York. Attached as Exhibit 1 is a photograph of the front of the residence.

The entrance to the SUBJECT PREMISES is located on the right side of the home off of the street level via stairs. The door entrance consists of two large glass doors. "30 Sidney Place" is written on a plaque in script to the left of the doors.

ATTACHMENT B

Property to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored

material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

16. Records and things evidencing the use of the Internet Protocol address 72.229.105.108, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

EXHIBIT 1